The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE

Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.

http://www.us-cert.gov/tlp/

DATE(S) ISSUED:

02/07/2017

SUBJECT:

Multiple Vulnerabilities in Google Android OS Could Allow for Remote Code Execution

OVERVIEW:

Multiple vulnerabilities have been discovered in the Google Android operating system (OS), the most severe of which could allow for remote code execution. Android is an operating system developed by Google for mobile devices, including, but not limited to, smartphones, tablets, and watches. These vulnerabilities could be exploited through multiple methods such as email, web browsing, and MMS when processing media files. Successful exploitation of the most severe of these vulnerabilities could result in remote code execution in the context of the application. Depending on the privileges associated with this application, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. If this application has been configured to have fewer user rights on the system, exploitation of the most severe of these vulnerabilities could have less impact than if it was configured with administrative rights.

THREAT INTELLIGENCE:

There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEM AFFECTED:

- Android OS builds utilizing Security Patch Levels prior to February 01, 2017.

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

TECHNICAL SUMMARY:

Google Android OS is prone to multiple vulnerabilities, the most severe of which could allow for remote code execution. The vulnerabilities are as follows:

- Remote code execution vulnerability in Surfaceflinger (CVE-2017-0405).

- Remote code execution vulnerability in Mediaserver (CVE-2017-0406, CVE-2017-0407).
- Remote code execution vulnerability in libgdx (CVE-2017-0408).
- Remote code execution vulnerability in libstagefright (CVE-2017-0409).
- Elevation of privilege vulnerability in Java.Net (CVE-2016-5552).
- Elevation of privilege vulnerability in Framework APIs (CVE-2017-0410, CVE-2017-0411, CVE-2017-0412).
- Elevation of privilege vulnerability in Mediaserver (CVE-2017-0415).
- Elevation of privilege vulnerability in Audioserver (CVE-2017-0416, CVE-2017-0417, CVE-2017-0418, CVE-2017-0419).
- Information disclosure vulnerability in AOSP Mail (CVE-2017-0420).
- Information disclosure vulnerability in AOSP Messaging (CVE-2017-0413, CVE-2017-0414).
- Information disclosure vulnerability in Framework APIs (CVE-2017-0421).
- Denial of service vulnerability in Bionic DNS (CVE-2017-0422).
- Elevation of privilege vulnerability in Bluetooth (CVE-2017-0423).
- Information disclosure vulnerability in AOSP Messaging (CVE-2017-0424).
- Information disclosure vulnerability in Audioserver (CVE-2017-0425).
- Information disclosure vulnerability in Filesystem (CVE-2017-0426).
- Remote code execution vulnerability in Qualcomm crypto driver (CVE-2016-8418).
- Elevation of privilege vulnerability in kernel file system (CVE-2017-0427).
- Elevation of privilege vulnerability in NVIDIA GPU driver (CVE-2017-0428, CVE-2017-0429).
- Elevation of privilege vulnerability in kernel networking subsystem (CVE-2014-9914).
- Elevation of privilege vulnerability in Broadcom Wi-Fi driver (CVE-2017-0430).
- Vulnerabilities in Qualcomm components (CVE-2017-0431).
- Elevation of privilege vulnerability in MediaTek driver (CVE-2017-0432).
- Elevation of privilege vulnerability in Synaptics touchscreen driver (CVE-2017-0433, CVE-2017-0434).
- Elevation of privilege vulnerability in Qualcomm Secure Execution Environment Communicator driver (CVE-2016-8480).
- Elevation of privilege vulnerability in Qualcomm sound driver (CVE-2016-8481, CVE-2017-0435, CVE-2017-0436).
- Elevation of privilege vulnerability in Qualcomm Wi-Fi driver (CVE-2017-0437, CVE-2017-0438, CVE-2017-0439, CVE-2016-8419, CVE-2016-8420, CVE-2016-8421, CVE-2017-0440, CVE-2017-0441, CVE-2017-0442, CVE-2017-0443, CVE-2016-8476).
- Elevation of privilege vulnerability in Realtek sound driver (CVE-2017-0444).
- Elevation of privilege vulnerability in HTC touchscreen driver (CVE-2017-0445, CVE-2017-0446, CVE-2017-0447).
- Information disclosure vulnerability in NVIDIA video driver (CVE-2017-0448).
- Elevation of privilege vulnerability in Broadcom Wi-Fi driver (CVE-2017-0449).
- Elevation of privilege vulnerability in Audioserver (CVE-2017-0450).
- Elevation of privilege vulnerability in kernel file system (CVE-2016-10044).
- Information disclosure vulnerability in Qualcomm Secure Execution Environment Communicator (CVE-2016-8414).
- Information disclosure vulnerability in Qualcomm sound driver (CVE-2017-0451).

Successful exploitation of the most severe of these vulnerabilities could result in remote code execution in the context of the application. Depending on the privileges associated with this application, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. If this application has been configured to have fewer user rights on the system, exploitation of

the most severe of these vulnerabilities could have less impact than if it was configured with administrative rights.

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate updates provided by Google Android or mobile carriers to vulnerable systems, immediately after appropriate testing.
- Run all software as a non-privileged user to diminish the effects of a successful attack.
- Remind users to download apps only from trusted vendors in the Play Store.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.

REFERENCES:
Google:
https://source.android.com/security/bulletin/2017-02-01.html

CVE:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-9914
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5552
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-8414
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-8418
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-8419
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-8420
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-8421
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-8476
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-8480
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-8481
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-10044
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0405
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0406
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0407
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0408
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0409
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0410
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0411
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0412
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0413
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0414
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0415
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0416
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0417
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0418
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0419
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0420
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0421

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0422
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0423
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0424
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0425
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0426
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0427
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0428
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0429
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0430
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0431
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0432
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0433
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0434
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0435
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0436
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0437
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0438
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0439
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0440
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0441
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0442
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0443
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0444
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0445
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0446
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0447
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0448
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0449
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0450
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0451